Enterprise Architecture Standard

Identity and Access Management (IdAM) Suite Standard
Reference Model Type and ID No: TRM 1.5.885.001
Status: Pending Approval
Analysis: (EA TRM)
Effective Date: XX/XX/20XX
Next Review Date: XX/XX/20XX
Approved By: Enterprise Architecture Standards Workgroup

Introduction

The purpose of the IdAM Suite Standard is to define the federated identity and access management software suites to be utilized by all departments exchanging authentication and authorization data between security domains within the California State government. The IdAM Suite Standard will enable web-based authentication and authorization interoperability functions including single sign-on (SSO), across sites that are hosted by multiple agencies.

Standardizing the exchange of security and authorization data between the agencies will assist in unifying disparate information systems and reduce costs associated with licensing and maintenance which will further the intent of Government Code 11545(b) (3) which is to minimize overlap, redundancy and cost in state operations by promoting the efficient and effective use of Information Technology (IT).

Standard Requirements

The IdAM Suite Standard authorizes the use of the IdAM suites provided by IBM, Oracle, and Microsoft.

Authorities

Section 11545 of the Government Code (b) The duties of the State Chief Information Officer shall include, but are not limited to, all of the following: (2) Establishing and enforcing state information technology strategic plans, policies, standards, and enterprise architecture.

Implementation

The IdAM Suite Standard is to be used for all exchange of authentication and authorization data between security domains within the California State government. The implementation of these products and the framework for providing a federated domain trust service is identified in the State Identity Credential and Access Management Roadmap and Implementation Guidelines included as EA Practice TRM 1.5.885.002 in Section 158A of the Statewide Information Management Manual.

Exceptions to this EA Standard may be submitted to the OCIO by following the "OCIO EA Compliance Component Instructions" in the Statewide Information Management Manual Section 58A, Enterprise Architecture Developers Guide.